

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1           **Claim 1 (currently amended):** A method for carrying  
2 out an electronic transaction across a communication  
3 network linking several entities; ~~this method is~~  
4 ~~characterised in that~~ comprising the following steps:  
5 a) a first entity builds a first message combining ~~all of~~  
6 ~~the~~ transaction data and calculates a first cryptogram  
7 of ~~this~~ said first message using a first key system  
8 that ~~[[it]]~~ said first entity shares with ~~[[the]]~~ a last  
9 (n<sup>th</sup>) entity; ~~this~~ said first entity then links a  
10 second message with ~~[[the]]~~ said first cryptogram and  
11 calculates a second cryptogram of ~~the whole~~ said  
12 second message linked with said first cryptogram using  
13 a second key system that ~~[[it]]~~ said first entity  
14 shares with ~~the last but one~~ an (n-1)<sup>th</sup> entity, and so  
15 on; ~~[[the]]~~ said first entity links an (n-1)<sup>th</sup> message  
16 with ~~[[the]]~~ an (n-2)<sup>th</sup> cryptogram previously obtained  
17 and calculates an (n-1)<sup>th</sup> cryptogram of ~~the whole~~ said  
18 (n-1)<sup>th</sup> message linked with said (n-2)<sup>th</sup> cryptogram  
19 using ~~[[the]]~~ an (n-1)<sup>th</sup> key system that ~~[[it]]~~ said  
20 first entity shares with ~~[[the]]~~ a second entity;  
21 ~~[[the]]~~ said first entity then sends ~~[[the]]~~ a last

22           calculated   cryptogram   across   the   communication  
23           network;  
24    b)    [[the]]said second entity receives ~~this~~ said last  
25           cryptogram, uses [[the]]an appropriate key system to  
26           extract [[this]]said (n-1)<sup>th</sup> message from [[the]]said  
27           (n-1)<sup>th</sup> cryptogram containing [[it]]said (n-1)<sup>th</sup>  
28           message, and sends [[the]]said remaining (n-2)<sup>th</sup>  
29           cryptogram to [[the]]a third entity, and so on;  
30           [[the]]said n<sup>th</sup> entity receives [[the]]said first  
31           cryptogram and uses [[the]]an appropriate key system  
32           to extract [[the]]said first message contained within  
33           [[it]]said first cryptogram.

1           **Claim 2 (original):** A method in accordance with claim  
2    1, whereby the communication network therefore only  
3    includes entities that share a key with a first entity; the  
4    transaction then takes place between this first entity,  
5    which is the message source, and the last entity, which is  
6    the message recipient.

1           **Claim 3 (original):** A method in accordance with claim  
2    1, whereby the communication network includes a first group  
3    of entities made up of a first entity and (i-1) others,  
4    each of which shares a key system with said first entity,  
5    and a second group of entities made up of a first entity  
6    that is the last entity of this first group, i.e. entity i,

7 and (n-i) others, and whereby entity i shares a key system  
8 with each of the (n-1) following entities, said method  
9 being made up of two successive stages:

10 a first stage, in which the message built by the first  
11 entity of the first group is sent to the  $i^{\text{th}}$  entity of the  
12 first group in accordance with operations a) and b) in  
13 claim 1;

14 a second stage, in which the message extracted by the  
15 first entity of the second group is sent to the last entity  
16 of the second group in accordance with said operations a)  
17 and b) in claim 1.

1 **Claim 4 (original):** A method in accordance with claim  
2 1, whereby the communications network is composed of a  
3 first group of entities made up of a first entity and (i-1)  
4 others that share a key system with said first entity, a  
5 second group of entities made up of a first entity that is  
6 the last entity of this first group and (j-i+1) others that  
7 share a key system with said first entity of this second  
8 group, a third group of entities made up of a first entity  
9 that is the last entity of said second group and (n-j)  
10 others, where the (n-j+1) entities of this third group  
11 share a key system with said first entity of the first  
12 group, this method being characterised in that:

13 the first entity of the first group performs  
14 operations a) set forth in claim 1, using the key systems

15     that it shares with all other entities in the first and  
16     third groups;

17             the entities in the first group process the  
18     cryptograms that they receive in accordance with operations  
19     b) set forth in claim 1;

20             the first entity of the second group performs  
21     operations a) set forth in claim 1, using the key systems  
22     that it shares with all other entities in this second  
23     group;

24             the entities in the second group process the  
25     cryptograms that they receive in accordance with operations  
26     b) set forth in claim 1;

27             the entities in the third group unencrypt the  
28     cryptograms that they receive in accordance with operations  
29     b) set forth in claim 1.

1             **Claim 5 (original):** A method in accordance with claim  
2     1, whereby a group's first entity, *i*, calculates a  
3     cryptogram of the messages intended for the group's other  
4     entities, *i*+1, *i*+2, ..., *j*, without encapsulating them, and  
5     whereby each entity *i*+1, *i*+2, ..., *j* receives and checks  
6     the message intended for it using its key system that it  
7     shares with *i*.

1           **Claim 6 (original):** A method in accordance with claim  
2   1, whereby the electronic transaction is a payment and  
3   whereby the entities are composed of cards (A), service  
4   points (P) capable of receiving said cards (A), service  
5   point concentrators equipped with a security module (MS)  
6   and connected to the service points and an issuer (E)  
7   responsible for issuing electronic payment cards and  
8   obtaining the electronic money, the communication network  
9   connecting service points (P) with the concentrators and  
10   said concentrators with the issuer, whereby each card (A)  
11   shares a key system  $K_{A,M}$  with a security module (MS), whereby  
12   each card A also shares a key system  $K_{A,E}$  with the issuer  
13   (E), and whereby each card (A) shares a key system  $K_{A,P}$  with  
14   a service point (P).

1           **Claim 7 (original):** A method in accordance with claim  
2   6, in which:  
3   a)   the card (A):  
4           calculates a message (M') intended for the issuer  
5           (E), whereby said message contains the running total  
6           of the amounts paid, the transaction number ( $NT_A$ ), the  
7           transaction number ( $NT_{MS}$ ) of the security module (MS)  
8           to which the service point is connected and the  
9           identifier of said security module ( $ID_{MS}$ ),

10               calculates a first cryptogram  $K_{A,E}(M')$  of said  
11               message using key system  $K_{A,E}$  that it shares with the  
12               issuer,  
13               adds a message (M) containing the transaction  
14               amount (m), running total, transaction numbers ( $NT_A$ ,  
15                $NT_{MS}$ ) and identifier ( $ID_{MS}$ ) to said first cryptogram,  
16               encapsulates the result in a second cryptogram  
17                $K_{A,M}(M, K_{A,E}(M'))$  using key system  $K_{A,M}$  that it shares  
18               with the security module (MS),  
19               adds message M to said second cryptogram,  
20               encapsulates the result in a third cryptogram  $K_S(M,$   
21                $K_{A,M}(M, K_{A,E}(M'))$ ) using key system  $K_{A,P}$ ,  
22               sends said third cryptogram to the service point  
23               (P),  
24       b)       said service point (P) uses key system  $K_{A,P}$  to  
25               decapsulate the cryptogram that it has received,  
26               retrieves and checks message M and records  
27                $K_{A,M}(M, K_{A,E}(M'))$ , and whereby the method is repeated if  
28               use of the service has not ended,  
29       c)       when the service session ends the service point (P)  
30               resends the last message  $K_{A,M}(M, K_{A,E}(M'))$  to the security  
31               module (MS),  
32       d)       said security module (MS) uses key system  $K_{A,M}$  to  
33               decapsulate the cryptogram that it has received,  
34               retrieves the message (M) and sends  $K_{A,E}(M')$  to the  
35               issuer,

36 e) said issuer (E) uses key system  $K_{A,E}$  to decapsulate the  
37 cryptogram that it has received and extracts the  
38 message (M') intended for it.